System for correction of three and four errors

Patent Number:	US5710782
Publication date:	1998-01-20
Inventor(s):	WENG LIH-JYH (US)
Applicant(s)::	QUANTUM CORP (US)
Requested Patent:	WO9724813
Application Number:	US19950580351 19951228
Priority Number (s):	US19950580351 19951228
IPC Classification:	H03M13/00
EC Classification:	H03M13/15P
Equivalents:	AU1346897, AU7681696, CA2213293, CN1176714, EP0830742 (WO9724813), JP11501795T, WO9724812

Abstract

A system determines the error locations of four errors in GF(22m) by transforming a degree-four error locator polynomial ultimately into two quadratic equations, finding the solutions of these equations, and from these solutions determining the roots of an error locator polynomial. The system first manipulates the error locator polynomial, which is of the form: sigma (x)= sigma 4x4+ sigma 3x3 sigma 2x2+ sigma 1x+ sigma 0 [1]into the form: theta (y)=y4+ theta 2y2+ theta 1y+ theta 0 [2]where the theta i's are combinations of the coefficients of the terms of the error locator polynomial. The system has thus produced an equation in which the coefficient of the y3 term is 0. The system then factors theta (y), to produce theta (y)=(y2+t*y+u)*(y2+v*y+w), [3]where "*" represents multiplication. It then determines the values of t, u, v and w by equating the coefficients of the two expressions for theta (y) and solving first for the variable t, which is equal to v, and then for the variables w and u. Once the values of the variables are determined, the system solves two quadratic equations, one for each of the factors of equation 3. Based on these solutions, the system determines the four error locations associated with the degree-four error locator polynomial.

(19)日本国特許庁（J P）　(12) 公表特許公報(A)　(11)特許出願公表番号

特表平11－501795

(43)公表日　平成11年(1999) 2月9日

(51)Int.Cl.⁶	識別記号	F I	
H 0 3 M　13/00		H 0 3 M　13/00	
G 1 1 B　20/18	5 3 2	G 1 1 B　20/18	5 3 2 D
	5 4 4		5 4 4 Z

審査請求　未請求　予備審査請求　未請求(全 34 頁)

(21)出願番号　特願平9－524507
(86) (22)出願日　平成8年(1996)12月18日
(85)翻訳文提出日　平成9年(1997) 8月27日
(86)国際出願番号　P C T／U S 9 6／2 0 5 4 7
(87)国際公開番号　W O 9 7／2 4 8 1 3
(87)国際公開日　平成9年(1997) 7月10日
(31)優先権主張番号　0 8／5 8 0，3 5 1
(32)優先日　1995年12月28日
(33)優先権主張国　米国（U S）
(81)指定国　E P(A T，B E，C H，D E，D K，E S，F I，F R，G B，G R，I E，I T，L U，M C，N L，P T，S E)，A U，C A，C N，J P，K R，S G

(71)出願人　クウォンタム・コーポレイション
アメリカ合衆国、95035　カリフォルニア州、ミルピタス、マッカーシー・ブールバード、500
(72)発明者　ウェン，リー－ジャ
アメリカ合衆国、01545　マサチューセッツ州、シュルーズベリー、ブルックデイル・サークル、95
(74)代理人　弁理士　深見　久郎　（外3名）

(54)【発明の名称】　3つおよび4つのエラーを訂正するための改良されたシステム

(57)【要約】
リードソロモン符号またはＢＣＨ符号のコードワード内の４つのエラーの位置を決定するための方法が開示される。四次エラーロケータ多項式が操作され（５００、５０２、５０４、５０６）三次の項の係数がゼロである形にされ、それから２つの二次多項式が生成される（５０８、５１０、５１４、５１６、５１８）。２つの二次多項式の解は次にエラー位置と関連付けられる（５２４）。２つの二次多項式を生成するためのステップ（５１４）において、立方根を決定するための回路（２００）が使用される。

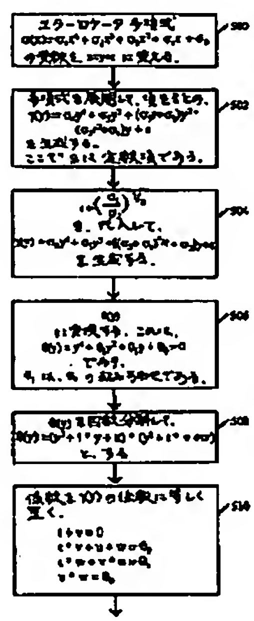

FIG. 5

【特許請求の範囲】

1．リードソロモン符号またはＢＣＨ符号のコードワード内の４つのエラーの位置を決定する方法であって、この方法は、

ａ．四次エラーロケータ多項式

$\sigma(X)=\sigma_4 X^4+\sigma_3 X^3+\sigma_2 X^2+\sigma_1 X^1+\sigma_0$

を操作して

$\theta\ \theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_2$

の形の多項式を生成するステップと、

ｂ．多項式を因数分解して、$\theta(y)=(y^2+t \cdot y+u) \cdot (y^2+v \cdot y+w)$にするステップと

、

ｃ．ステップａおよびステップｂの多項式の係数を等置するステップと、

$t+v=0$

$t \cdot v+u+w=\theta_2$

$t \cdot w+v \cdot u=\theta_1$

$u \cdot w=\theta_0$；

ｄ．唯一の未知数ｔを持つ方程式

$t^3+\theta_2 t+\theta_1=0$

を決定するステップと、

ｅ．解t_0について解くステップと、

ｆ．ｕおよびｗを解とする二次方程式を形成するステップと、

$p^2+(\theta_2+t_0^2)p+\theta_0=0$

ｇ．解p_0およびp_1について解くステップと、

ｈ．解を$\theta(y)$に代入して１対の二次方程式の解を決定するステップと、

$y^2+t_0 \cdot y+p_1=0$

$y_2+t_0 \cdot y+p_1=0$;

ｉ．１対の二次方程式の解y_0、y_1およびy_2、y_3を、四次エラーロケータ多項式の解と関連付けるステップと、

ｊ．四次エラーロケータ多項式の解をコードワード内の位置と関連付けるステップとを含む、コードワード内の４つのエラーの位置を決定する方法。

2、$t^3+\theta_2 t+\theta_1=0$の解について解くステップは、

i．変数を$t=z+\frac{a}{z}$ここで$a=\theta_2$に変えて、$z^3+\frac{a^3}{z^3}+\theta_1=0$の形の方程式を生成するステップと、

ii．ステップiの方程式をz^3で乗して、変数z^3を持つ二次方程式を得るステップと、

$(z^3)^2+\theta_1 z^3+a^3=0$

iii．ステップiiの二次方程式をz^3について解くステップと、

iv．z^3の立方根z_0を決定するステップと、

v．z_0の値を式$t=z+\frac{a}{z}$に代入するステップとを含む、請求項1に記載の方法。

3．エラーロケータ多項式を$\theta(y)$に変換するステップは、

i．変数を$x=y+r$ここで$r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$に変え、項を展開しまとめて

$\gamma(y)=\sigma_4 y^4+\sigma_3 y^3+(\sigma_3 r+\sigma_2)y^2+(\sigma_3 r^2+\sigma_1)y+\sigma_4 r^4+\sigma_3 r^3+\sigma_2 r^2+\sigma_1 r+\sigma_0=0$

の形の方程式を生成するステップと、

ii．$r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$をステップiの方程式に代入し、

$\gamma(y)=\sigma_4 y^4+\sigma_3 y^3+\left[(\sigma_3 * \sigma_1)^{1/2}+\sigma_2\right]y^2+s$

の形の方程式を生成するステップを含み、ここでsはステップiの方程式の定数項であり、さらに、

iii．

$\theta\theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_2=0$

ここで

$$\theta\theta_1 = \frac{(\sigma_3 * \sigma_1)^{1/2} + \sigma_2}{s}$$

$$\theta\theta_1 = \frac{\sigma_1}{s} \text{かつ}$$

$$\theta\theta_0 = \frac{\sigma_4}{s}$$

に展開される、

$$\theta\theta(y) = \frac{y^4 * \gamma\left(\frac{1}{y}\right)}{s}$$

の解を求めるステップとを含む、請求項1に記載の方法。

4．リードソロモン符号またはＢＣＨ符号のコードワード内の４つのエラーの位置を決定する方法であって、

ａ．四次エラーロケータ多項式

$\sigma(x)=\sigma_4 x^4+\sigma_3 x^3+\sigma_2 x^2+\sigma_1 x^1+\sigma_0$

を操作して、

$\theta\theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_2$

の形の多項式を生成するステップと、

ｂ．多項式を、因数分解して$\theta(y)=(y^2+t^* y+u)^*(y^2+v^* y+w)$にするステップと

、

ｃ．ｔ、ｕ、ｖ、およびｗの値を決定するステップと、

ｄ．値ｔ、ｕ、ｖ、およびｗを$\theta(y)$に代入し、１対の二次方程式の解を決定するステップと、

$y^2+t^* y+u=0$

$y^2+v^* y+w=0$;

ｅ．１対の二次方程式の解y_0、y_1およびy_2、y_3を、四次エラーロケータ多項式の解と関連付けるステップと、

ｆ．四次エラーロケータ多項式の解をコードワード内の位置と関連付けるステップとを含む、コードワード内の４つのエラーの位置を決定する方法。

5．t、u、v、およびwの値を決定するステップは、

i．ステップaおよびステップbの多項式の係数を等置するステップと、

$t+v=0$

$t \cdot v+u+w=\theta_2$

$t \cdot w+v \cdot u=\theta_1$

$u \cdot w=\theta_0$

ii．唯一の未知数tを持つ方程式を決定するステップと、

$t^3+\theta_2 t+\theta_1=0$

iii．解t_0について解くステップと、

iv．uおよびwを解とする二次方程式を形成するステップと、

$p^2+(\theta_2+t_0^2)p+\theta_0=0$

v．uおよびwである解p_0およびp_1について解くステップとを含む、請求項4に記載の方法。

6．$t^3+\theta_2 t+\theta_1=0$の解について解くステップは、

a．変数を$t=z+\frac{a}{z}$ここで$a=\theta_2$に変え、$z^3+\frac{a^3}{z^3}+\theta_1=0$の形の方程式を生成するステップと、

b．ステップaの方程式をz^3で乗してz^3を変数とする二次方程式を得るステップと、

$(z^3)^2+\theta_1 z^3+a^3=0$

c．ステップbの二次方程式をz^3について解くステップと、

d．z^3の立方根z_0を決定するステップと、

e．z_0の値を式$t=z+\frac{a}{z}$に代入するステップとを含む、請求項5に記載の方法。

7．エラーロケータ多項式を$\theta(y)$に変換するステップは、

i．変数を$x=y+r$、ここで$r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$に変え、項を展開しまとめて、

$\gamma(y)=\sigma_4 y^4+\sigma_3 y^3+(\sigma_3 r+\sigma_2)y^2+(\sigma_3 r^2+\sigma_1)y+\sigma_4 r^4+\sigma_3 r^3+\sigma_2 r^2+\sigma_1 r+\sigma_0=0$

の形の方程式を生成するステップと、

ii. $r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$ をステップｉの方程式に代入し、

$\gamma(y)=\sigma_4 y^4+\sigma_3 y^3+\left[(\sigma_3 {*}\sigma_1)^{1/2}+\sigma_2\right]y^2+s$、の形の方程式を生成するステップ

とを含み、ここでｓはステップｉの方程式の定数項であり、さらに

iii. 展開すると、

$\theta\theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_2=0$

ここで

$$\theta\theta_2=\frac{(\sigma_3 {*}\sigma_1)^{1/2}+\sigma_2}{s}$$

$$\theta\theta_1=\frac{\sigma_1}{s}\text{ かつ}$$

$$\theta\theta_0=\frac{\sigma_0}{s}$$

となる、$\theta\theta(y)=\dfrac{y^4{*}\gamma\left(\frac{1}{y}\right)}{s}$

の解を求めるステップとを含む、請求項４に記載の方法。

【発明の詳細な説明】

３つおよび４つのエラーを訂正するための改良されたシステム

発明の分野

この発明は、一般に、データ処理システムに関し、より特定的には、エラー訂正コードを用いたデータにおけるエラーを復号しかつ訂正するためのシステムに関する。

発明の背景

磁気ディスクなどの磁気媒体上に記憶されたデータは、典型的には、符号化された形で記憶されており、したがって記憶されたデータ内のエラーを恐らくは訂正することができる。エラーは、たとえば、符号間干渉、ディスク内の欠陥、またはノイズによって起こり得る。ディスク上に記憶されるデータの密度が増加するに伴い、より多くのエラーが起こりかねず、システムはより多数のエラーを訂正せねばならない。システムがエラーを訂正する速度は、システムがデータを処理する全体的な速度において重要である。

記憶する前に、多ビットデータシンボルはエラー訂正コード（ＥＣＣ）を用いて符号化される。データシンボルがディスクから検索され復調されるとき、ＥＣＣが用いられ、その名前が示しているように誤ったデータを訂正する。

特定的には、ｋ個のデータシンボルの列はディスクに書込まれる前に、（ｎ，ｋ）ＥＣＣを用いて数学的に符号化され、ｎ－ｋ　ＥＣＣシンボルを形成する。ＥＣＣシンボルは次にデータの列に添えられｎ－シンボルエラー訂正コードワードを形成し、これは次にディスクに書込まれるかまたはディスク上に記憶される。データがディスクから読出されるとき、データシンボルおよびＥＣＣシンボルを含むコードワードは検索されそして数学的に復号される。復号の間、データ内のエラーは検出されそしてもし可能ならば、ＥＣＣシンボルの操作によって訂正される（復号についての詳細な説明に関しては、ピーターソン(Peterson)およびウェルドン(Weldon)の『エラー訂正コード(Error Correction Codes)』第２版、MIT 出版、1972を参照）。

データシンボルの列の中の多数のエラーを訂正するためには、システムは典型

的には、ガロア体として知られる数組のシンボルのさまざまな数学的特性を効率的かつ効果的に利用するＥＣＣを用いる。ガロア体は、「ＧＦ（P^m）」と表わされ、「Ｐ」は素数であり、「ｍ」は体の中の各要素またはシンボル内の基数「Ｐ」の桁数と考え得る。Ｐは普通デジタルコンピュータおよびディスクドライブアプリケーションにおいては値２をとり、したがって、ｍは各シンボル内のビット数である。一般にガロア体とともに使用されるＥＣＣは、リードソロモン符号またはＢＣＨ符号である。

リードソロモン符号またはＢＣＨ符号の改変されたコードワードの復号には本質的に４つの主要ステップがある。システムはまずＥＣＣシンボルの操作の結果に基づいたエラーシンドロームを決定する。次に、エラーシンドロームを用いて、システムはエラーロケータ多項式を決定する。これはエラーの数と同じ数の次数を有する多項式である。システムは次にエラーロケータ多項式の解を求め、各解からコードワード内の関連するエラーの位置を決定する。最後に、システムはエラー位置に対するエラー値を求める。デジタルコンピュータなどの２進システムにおいてはエラー位置に対して可能なエラー値は１つしかないので、エラー値を決定するステップは重要ではない。

エラー訂正処理の中で最も時間を費やすのは、シンドロームを決定し、エラー位置を求めるステップである。ここに説明する発明は、３つまたは４つのエラーの位置を求めるためにエラー訂正システムの費やす時間を減じる。これは、三次および四次のエラーロケータ多項式の解を求めることを含む。

先行のシステムにおいては、四次の多項式の解は、試行錯誤またはマトリックス操作もしくはルックアップテーブルによって決定されている。試行錯誤法は、あらゆる可能な値、すなわちコードワード位置に関連する適用可能なＧＦ（2^{2m}）のすべての要素を多項式に代入し、各値について多項式の数値を求めることによって行なわれる。もし所与の値について多項式がゼロに等しければ、その値が解である。このシステムは、次に可能な値を多項式に代入しその値が解がどうかを判断することによってこの試行錯誤処理を続け、すべての可能な値が試されてしまうかまたはすべての４つの解が決定されるまでこれを続ける。この試行錯誤処理は、最適化された形態では通常チェンサーチとして知られているが、時間

のかかるものである。さらに、コードワード内のエラーの位置によって処理に費やされる時間が変化するために、処理にかかる時間を予測することができない。

マトリックス操作およびルックアップテーブル法は、

$\sigma_4 X^4+\sigma^3 X_3+\sigma^2 X_2+\sigma_1 X+\sigma_0$

の形の一般四次多項式を変換して、

x^4+x^2+ax+b

の形の多項式にすることを含んでいる。

ルックアップテーブルが使用されるのならば、テーブルは、ａおよびｂの可能な値のすべての組に対しての解の組を含んでいる。今日使用されている典型的にはＧＦ（2^8）にわたるＥＣＣについては、テーブルは2^{16}のエントリを有し、その各々が３２ビットすなわち４つの８ビット要素を有する。したがって、テーブルはかなりの量の記憶空間を占め、比較的複雑なアドレッシング機構を必要とする。

マトリックス操作法を用いたシステムは、$f(\alpha),f(\alpha^1),f(\alpha^2),...f(\alpha^{m-1})$で、ここで$f(x)=x^4+x^2+ax+b$であるものを決定することにより、ｍ×ｍのマトリックスを生成する。次に、マトリックスを操作してマトリックスによって広がりが規定される空間のナル空間を決定する。多項式の解は次にナル空間にわたるベクトルから得ることができる（より詳細な説明については、Ｅ・Ｒ・ベールカンプ(Berlekamp)『代数的コード理論(Algebraic Coding Theory)』、マグロウヒルブックカンパニー(McGraw Hill Book Company)、1968 年を参照）。この方法では、ｍ×ｍのマトリックスのビット毎の操作が必要となり、典型的にはマトリックスを変換するために多くの操作演算が必要である。したがって、この方法は時間がかかりかつ計算に集中している。

ここで説明するこの発明のシステムは、４つのエラー位置を求めるためにかかる時間を減じ、四次多項式の解を決定することを含む。このシステムは、ベールカンプによって『代数的コード理論』に説明されているような二次多項式の解を決定する周知の方法を利用している。さらに、このシステムは、ファンデルホルスト(Van der Horst)およびバーガー(Berger)によって「三重エラー訂正２進ＢＣＨコードの完全なデコーディング(Complete Decodjng of Triple-Error-

Correcting Binary BCH Codes)」、『情報理論についての IEEE 紀要(IEEE Transactions on Information Theory)』、Vol.IT–22、1976 年、138 頁から147頁に説明されている三次多項式の解を決定する方法を利用している。

ファンデルホルストおよびバーガーの教示に従って三次多項式の解を求めるためには、ＧＦ（2^{2m}）にわたってのガロア体要素の立方根を決定することが必要である。後にここで説明するように、本発明者は比較的迅速かつ容易に立方根を求めるためのある発明の回路を開発した。

発明の概要

この発明は、四次エラーロケータ多項式を最終的に２つの二次方程式に変換し、これらの方程式の解を求め、これらの解からエラーロケータ多項式の解を決定することによって、ＧＦ（2^{2m}）内の４つのエラーのエラー位置を決定するシステムである。

より特定的には、このシステムは、最初に四次多項式

$$\sigma(x)=\sigma_4 x^4+\sigma_3 x^3+\sigma_2 x^2+\sigma_1 x+\sigma_0$$

［1］

を操作して、

$$\theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_0$$

［2］

の形にする。ここで、θ_1はエラーロケータ多項式の項の係数の組合せである。y^3の項の係数がゼロであることに注意されたい。

このシステムは次に$\theta(y)$を因数分解して、

$$\theta(y)=(y^2+t\cdot y+u)\cdot(y^2+v\cdot y+w),$$

［3］

にし、ここで「$\cdot$」は乗法を表わし、そしてこの式を展開して、

$$\theta(y)=y^4+(t+v)y^3+(t\cdot v+u+w)y^2+(t\cdot w+v\cdot u)y+u\cdot w.$$

［4］

にし、ここでｔ、ｕ、ｖ、およびｗは未知数である。式２および式３の係数を等置して、このシステムは、

$t+v=0$

$t\cdot v+u\cdot w=t^2+u\cdot w=\theta_2$

［5］

$t\cdot w+u\cdot v=t+w+t\cdot u=t\cdot(w+u)=\theta_1$

$u\cdot w=\theta_0$

と決定する。

このシステムは次に変数ｔを唯一の未知数とする方程式を生成する。

$t^3+\theta_2 t+\theta_1=0$

［6］

この三次方程式は以下により詳細に説明するように、ファンデルホルストおよびバーガーによって説明されている方法を用いて解くことができる。

一旦方程式６の解t_0が決定されると、この解はθ_1についての式に代入され、そしてこの式およびθ_0についての式を用いてｕおよびｗを解とする二次方程式が形成される。

$p^2+(\theta_2+t_0{}^2)p+\theta_0=0$

［7］

このシステムは次に二次多項式を解くためのベールカンプの方法を用いて、方程式７の解p_0およびp_1を求める。解p_0およびp_1はそれぞれｕおよびｗであるが、多項式３に代入され、各項はゼロとされ、２つの二次方程式が生成される。

$y^2+t_0\cdot y+p_0=0$

［8］

$y^2+t_0\cdot y+p_1=0$

ベールカンプ法を用いて決定される方程式８の解はまた、$\theta(y)$の解でもあり、したがってエラーロケータ多項式の解を生成するために直接用いることができる。

この直接的解法は、４つの解を求める、先行の試行錯誤またはマトリックス操作法よりも迅速である。さらに、他の先行の既知のシステムにおいて必要とされるように大きなルックアップテーブルを記憶したりそこにエントリしたりすることは必要ない。

図面の簡単な説明

この発明の性質および目的をより完全に理解するために、添付された図面に関連する以下の詳細な説明を参照されたい。図面中では、

図1は、この発明により構築されるデコーダの機能ブロック図である。

図2は、GF（2^{2m}）要素の立方根を決定するための発明の回路の機能ブロック図である。

図3は、図2の回路の動作のフローチャートである。

図4は、GF（2^8）についての図2の回路である。

図5は、図1のデコーダが4つのエラーの位置を決定するときに行なう動作のフローチャートである。

好ましい実施例の説明

ここで説明する加減乗除の数学演算は、GF（2^{2m}）にわたってのガロア体の演算である。

次に図1を参照すると、デコーダ10はシンドローム発生器12を含み、これは、従来の態様でエラーシンドロームの関連する組を生成するために動作する。もしシンドロームがすべてゼロであれば、シンドローム発生器12はコードワードにエラーはないと判断する。そうでなければ、シンドローム発生器はシンドロームをエラーロケータ多項式発生器14に送り、これは従来の態様でシンドロームから次数「e」のエラーロケータ多項式を生成する。ここでeはコードワード内のエラーの数である。エラーロケータ多項式発生器14は次にエラーロケータ多項式をエラーロケータプロセッサ16に送り、これはエラーロケータ多項式の解、すなわちエラー位置を決定するための適切な処理を選択しかつ実施する。図1は、これらの処理をいくつかのブロックまたはプロセッサとして描いている。つまり、1つのエラー位置を決定するためのプロセッサ18、2つのエラー位置を決定するためのプロセッサ20、3つのエラー位置を決定するためのプロセッサ22、4つのエラー位置を決定するためのプロセッサ24、および4つより多くのエラー位置を決定するためのプロセッサ26である。

2つ、3つ、および4つのエラープロセッサ20、22および24は相互接続

されている。以下に説明するように、エラーロケータプロセッサ１６は対応するエラーロケータ多項式を最終的に関連する二次方程式の組に変換することによって３つおよび４つのエラー位置を決定するためにかかる時間を減する。そのために、４つのエラープロセッサ２６は３つのエラープロセッサ２４および２つのエラープロセッサ２２の両者を利用する。同様に、３つのエラープロセッサ２４は２つのエラープロセッサ２２を利用する。これらの処理は、別個の専用プロセッサ内で起こっているように描かれているが、１つまたは２つ以上の多目的プロセッサ内で行なわれてもよい。

エラーロケータプロセッサ１６は、従来の態様で１つおよび２つのエラーの位置を決定する。これは、ファンデルホルストおよびバーガーによって説明される方法によって３つのエラーの位置を決定する。しかしながら、これは、ガロア体要素の立方根を決定する必要なステップを行なうために発明の回路を使用する。この回路および３つのエラーの位置を決定するための方法が、図２および図３を参照し以下に説明される。

エラーロケータプロセッサ１６は、図４を参照して以下に説明される独特の処理を用いて４つのエラーの位置を決定する。この処理を説明する前に、２つのエラー位置処理および３つのエラー位置処理がそれぞれＡ節およびＢ節で説明される。

Ａ．２つのエラー位置の決定

もしコードワードが２つのエラーを含んでいたならば、エラーロケータ多項式の形は、

$$\sigma(x)=\sigma_2 x^2+\sigma_1 x+\sigma_0 x$$

［１］

となる。この多項式の解を求めるために、このシステムは多項式をゼロに等しいとおく。

$$\sigma(x)=\sigma_2 x^2+\sigma_1 x+\sigma_0 x=0$$

［２］

そしてこの方程式を解x_0およびx_1について解く。

方程式２を解くためにエラーロケータプロセッサ１６はこの方程式の形を変換

する。

$y^2+y+C=0$

［3］

変数を、

$$x=\frac{\sigma_1}{\sigma_2}y$$

［4］

と変えることによって、方程式２は、

$$\sigma\sigma\left(\frac{\sigma_1}{\sigma_2}y\right)=\frac{\sigma_1^2}{\sigma_2}y^2+\frac{\sigma_1^2}{\sigma_2}y+\sigma_0$$

となる。次に、これを$\frac{\sigma_2}{\sigma_1^2}$で除することによって、このシステムは次の方程式を生成する。

$$y^2+y+\frac{\sigma_0\sigma_2}{\sigma_1^2}=0$$

［5］

したがって、方程式３のCは$\frac{\sigma_0\sigma_2}{\sigma_1^2}$である。

方程式５の解がGF（2^{2m}）内に存在するためには、方程式の両辺の「トレース」は同じでなくてはならない。トレースは、

$$\text{トレース}(\alpha')=\sum_{k=0}^{2m-1}(\alpha')^{2^k}$$

［6］

と定義される。

トレース（０）は０に等しく、したがって、解がガロア体内に存在するためには、

$$\text{トレース}\left[y^2+y+C\right]=0$$

［7］

である。項の合計のトレースは、個々の項のトレースの合計に等しい。ＧＦ（2^{2m}）においては、トレース(y^2)=トレース(y)であり、これらの和はガロア体和法を用いると、ゼロである。したがって、方程式５はもしトレース（Ｃ）＝０ならばＧＦ（2^{2m}）内に解を有する。

方程式５の一般解は、２ｍ－１個の「基底解」の線形結合である。基底解とは、ガロア体の「基底要素」C_1，$C_2 \cdots C_{2m-1}$の１つをＣとする方程式３の解である。基底要素とは、線形結合させると体のすべての他の要素を生成することができる体の要素である。これらの要素は、たとえば、各々が２ｍ－１個の０と１つの１とを含む、すなわちα^{i}=000...1 からα^{j}=100...00 である２ｍ－１個の要素の組であってもよい。このような体においては、Ｃ=00110...0は基底要素00100...0 と00010...0 との線形結合である。方程式５の一般解は、合計すると

$\frac{\sigma_0\sigma_2}{\sigma_1^2}$を生成する基底要素に対応する基底解の線形結合である。

生成元多項式X^4+X+1で定義されるＧＦ（2^4）においては、ゼロのトレースを有する各要素α^{i}はまたその最も重要なビットとしてゼロを有する。したがって、この体内の問題のＣは基底要素α^0=0001、α^1=0010 およびα^2=0100 の結合である。対応する基底解は、

$(\alpha^5)^2+\alpha^5=\alpha^0$　　ここで$y_0=\alpha^5$

$(\alpha^9)^2+\alpha^9=\alpha^1$　　ここで$y_0=\alpha^9$

$(\alpha^3)^2+\alpha^3=\alpha^2$　　ここで$y_0=\alpha^3$

であり、もう１つの基底解の組は、

$(\alpha^{10})^2+\alpha^{10}=\alpha^0$　　ここで$y_1=\alpha^{10}$

$(\alpha^7)^2+\alpha^7=\alpha^1$　　ここで$y_1=\alpha^7$

$(\alpha^{14})^2+\alpha^{14}=\alpha^2$　　ここで$y_1=\alpha^{14}$

である。このガロア体内では、たとえば、Ｃがα^8=0101 に等しい方程式３の解は、Ｃを

$C=\alpha^0+\alpha^2$=0001+0100

に分解し、基底解の対応する組を合計し、たとえば、

$y_0 = \alpha^{5} + \alpha^{3} = \alpha^{11}$

として第１の解を生成し、第２の解を、

$y_1 = y_0 + \alpha^{0}$

と決定することによって決定される。次に、このシステムは二次エラーロケータ多項式の解を、

$$x_0 = y_0\left(\frac{\sigma_1}{\sigma_2}\right)$$

$$x_1 = y_1\left(\frac{\sigma_1}{\sigma_2}\right)$$

として決定する。

<u>B．３つのエラー位置の決定</u>

３つのエラーに関連するエラーロケータ多項式の形は、

$\sigma(x) = \sigma_3 x^3 + \sigma_2 x^2 + \sigma_1 x + \sigma_0$

［８］

である。解を求めるために、このシステムは、多項式をゼロに等しいとおく。

$\sigma(x) = \sigma_3 x^3 + \sigma_2 x^2 + \sigma_1 x + \sigma_0 = 0$

［９］

そしてこの方程式の形を変換して、

$y^3 + ay + b = 0$

とする。このために、システムは変数を変え、

$$x = y + \frac{\sigma_2}{\sigma_3}$$

として、方程式９は、

$$\sigma\left(y + \frac{\sigma_2}{\sigma_3}\right) = \sigma_3\left(y + \frac{\sigma_2}{\sigma_3}\right)^3 + \sigma_2\left(y + \frac{\sigma_2}{\sigma_3}\right)^2 + \sigma_1\left(y + \frac{\sigma_2}{\sigma_3}\right) + \sigma_0 = 0$$

［10］

となる。次にシステムは方程式１０の項を展開して、

$$\sigma_3\left(y^3+y^2\frac{\sigma_2}{\sigma_3}+y\left(\frac{\sigma_2}{\sigma_3}\right)^2+\left(\frac{\sigma_2}{\sigma_3}\right)^3\right)+\sigma_2\left(y^2+\left(\frac{\sigma_2}{\sigma_3}\right)^2\right)+\sigma_1\left(y+\frac{\sigma_2}{\sigma_3}\right)+\sigma_0=0$$

とし、同類項をまとめて、

$$\sigma\sigma_3 y^3+(\sigma_2+\sigma_2)y^2+\left(\frac{\sigma_2^2}{\sigma_3}+\sigma_1\right)y+\frac{\sigma_2^3}{\sigma_3^2}+\frac{\sigma_2^3}{\sigma_3^2}+\frac{\sigma_1\sigma_2}{\sigma_3}+\sigma_0=0$$

[11]

を生成する。ＧＦ（2^{2n}）においては、同一項の合計はゼロに等しいので、方程式は、

$$\sigma\sigma_3 y^3+0y^2+\left(\frac{\sigma_2^2}{\sigma_3}+\sigma_1\right)y+0+\frac{\sigma_1\sigma_2}{\sigma_3}+\sigma_0=0$$

[12]

となる。このシステムは方程式１２をσ_3で除し、次の形の方程式を生成する。

$y^3+ay+b=0$

[13]

$$\text{ここで } a=\frac{\sigma_2^2}{\sigma_3^2}+\frac{\sigma_1}{\sigma_3}\quad\text{かつ } b=\frac{\sigma_0}{\sigma_3}+\frac{\sigma_1\sigma_2}{\sigma_3^2}.$$

もしａ≠０ならば、システムは変数を変え、

$$y=z+\frac{a}{z}$$

[14]

とし、方程式１３は、

$$\left(z+\frac{a}{z}\right)^3+a\left(z+\frac{a}{z}\right)+b=0$$

[15]

となる。次に方程式１５を展開し同類項をまとめて、

$$z^3+\frac{a}{z}z^2+\left(\frac{a}{z}\right)^2 z+\left(\frac{a}{z}\right)^3+az+\frac{a^2}{z}+b=z^3+az+\frac{a^2}{z}+\frac{a^3}{z^3}+az+\frac{a^2}{z}+b=$$

$$z^3+\frac{a^3}{z^3}+b=0.$$

[16]

を生成する。このシステムは次に方程式１６をz^3で乗じて、

$$(z^3)^2+bz^3+a=0,$$

[17]

を生成し、この式は、変数z^3を有する二次方程式である。次に方程式１７はＡ節で説明した２つのエラー方法を用いて解くことができる。

一旦１つの解z_{03}が決定されると、このシステムは以下に図２および図３を参照して説明される回路を用いて立方根z_0を求める。ｍが偶数である限り、方程式１７の第２の解z_1は、

$$z_1=z_0 * \alpha\alpha^{\frac{2^{2m}-1}{3}}$$

であり、ｍは偶数であるので$2^{2m}-1$は３で割り切れるので、指数$\frac{2^{2m}-1}{3}$は常に整数である。方程式１７の第３の解は、

$$z_2=z_1+z_0$$

である。このシステムは次にこれらの解をｙについて式に代入し、代入の結果を個々に$\frac{\sigma_2}{\sigma_3}$に加えて、三次エラーロケータ多項式の解$x_0$、$x_1$および$x_2$を生成する。

もしａ＝０ならば、方程式１３の解は$y=b^{1/3}$である。ｂの立方根を求めるために、このシステムは図２に示す回路を使用する。一旦立方根がわかれば、このシステムはy_1およびy_2を、

$$y_1=y_0 * \alpha\alpha^{\frac{2^{2m}-1}{3}} \quad \text{および}$$
$$y_2=y_0+y_1$$

と決定し、これらの値から解x_0、x_1およびx_2を決定する。

次に図2および図3を参照すると、回路200は、GF（2^{2m}）の要素α^{3k}の立方根を、この要素を．α^{2k}に関連する累乗で乗することによって求める。いずれのGF（2^{2m}）の要素の2^k乗も、複数の従来のガロア体乗算器を使用して容易に達成される。

回路200は、恒等式$x^2-1=(x-1)^*(x+1)$を利用している。xが2^mに等しいと、この恒等式は、$2^{2m}-1=(2^m-1)^*(2^m+1)$となる。因子$2^m-1$または$2^m+1$の1つは3で割り切れるが、両方の因子が割り切れるわけではない。もしたとえば、m＝4であれば、因子2^m-1は3で割り切れ、2^m+1は割り切れない。回路200はまた$\left(\alpha^{2m-1}\right)^*\left(\alpha^{2m+1}\right)=\alpha^{2m+1}$という事実も利用している。

回路200を用いて、ガロア体要素α^{3k}は、乗算器202内で、3で割り切れない恒等式の因子に対応する累乗に乗される（ステップ300）。m＝4の例では、要素は、2^m+1乗に乗される。そして、ルックアップテーブル204を用いて、積$\alpha^{3k(2^m+1)}$の立方根$\alpha^{k(2^m+1)}$を求める（ステップ302）。可能な積$\alpha^{3k(2^m+1)}$の立方根についてしかエントリを持たないテーブルは、比較的小さい。GF（2^8）の例では、テーブルは5つのエントリしか持たない。

乗算器202はまた、要素α^{3k}を$\dfrac{2^m-1}{3}$に対応する累乗で乗し（ステップ304）、その結果は、ルックアップテーブル204によって生成された立方根で、GF乗算器206内で乗される（ステップ306）。

$$\alpha^{k(2^m+1)}*\alpha^{k(2^m-1)}=\alpha^{k(2^{2m})}$$

ステップ308において、このシステムは、この積を$\dfrac{1}{2^{m+1}}$乗し、立方根α^kを生成する。

図4は、GF（2^8）、すなわちm＝4についての回路200を示している。α^{3k}を2^m+1乗するために、この回路は、GF乗算器201内で、まず要素を

2^mまたは2^4＝１６乗する。次に、ＧＦ乗算器２０３内で、積$\alpha^{3k(16)}=\alpha^{48k}$を要

素α^{3k}で乗して、積$\alpha^{3k(2^m+1)}=\alpha^{51k}$を生成する。この積は、５つの要素のルックアップテーブル２０４に入るために使用される。

$\alpha^{0} \rightarrow \alpha^{0}$

$\alpha^{51} \rightarrow \alpha^{17}$

$\alpha^{102} \rightarrow \alpha^{34}$

$\alpha^{153} \rightarrow \alpha^{51}$

$\alpha^{204} \rightarrow \alpha^{68}$

これによってα^{17k}が生成される。

ＧＦ乗算器２０７および２０８を用いて、要素α^{3k}は$\left(\frac{2^m-1}{3}\right)$または$\frac{2^4-1}{3}=5$

乗される。ＧＦ乗算器２０７はまず要素を2^2または４乗し、ＧＦ乗算器２０９

は積$\alpha^{3k(4)}=\alpha^{12k}$を要素$\alpha^{3k}$で乗し、積$\alpha^{15k}$を生成する。

ＧＦ乗算器２０６は次に２つの積を乗する$\alpha^{17k}\cdot\alpha^{15k}=\alpha^{32k}$。この結果は次に

乗算器２１０内で$\frac{1}{2^{m+1}}$または$\frac{1}{2^5}=\frac{1}{32}$乗され、立方根、$\alpha^k$を生成する。

回路２００は、そこに与えられたすべての要素に対して結果を生成する。しかしながら、ガロア体のすべての要素に対する立方根が必ずしもあるわけではない。したがって、このシステムは結果をテストして（ステップ３１０）、その結果が実際の立方根であるかどうかを判断せねばならない。したがってこのシステムは、結果をそれ自身で２回乗し、その積が回路に与えられた要素と等しいかどうかを判断する（ステップ３１２）。もし等しければ、立方根は正確であり、エラー位置が決定できる（ステップ３１４）。しかしながらもし積が要素に等しくなければ、システムはエラー位置が見つからないと判断する（ステップ３１６）。そしてシステムはエラー位置を探す処理を終了する。

Ｃ．４つのエラー位置の決定

４つのエラーに関連するエラーロケータ多項式の形は、

$\sigma(x)=\sigma_4 x^4+\sigma_3 x^3+\sigma_2 x^2+\sigma_1 x+\sigma_0$

[18]

である。解を求めるため、システムはこの多項式をゼロに等しいとおく。

$\sigma(x)=\sigma_4 x^4+\sigma_3 x^3+\sigma_2 x^2+\sigma_1 x+\sigma_0=0$

[19]

そしてこの方程式の形を変換し、

$y^4+dy^2+ey+h=0$

とする。特定的には、ここで図５を参照すると、システムはステップ５００において変数を変える。

$$x=y+r,\quad ここで\quad r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$$

そして方程式１９は

$\gamma(y)=\sigma_4(y+r)^4+\sigma_3(y+r)^3+\sigma_2(y+r)^2+\sigma_1(y+r)+\sigma_0=0$

[20]

となる。ステップ５０２においてこのシステムは項を展開して、

$\gamma(y)=\sigma_4(y^4+r^4)+\sigma_3(y^3+y^2r+yr^2+r^3)+\sigma_2(y^2+r^2)+\sigma_1(y+r)+\sigma_0=0$

とし、同類項をまとめて、

$\gamma(y)=\sigma_4 y^4+\sigma_3 y^3+(\sigma_3 r+\sigma_2)y^2+(\sigma_3 r^2+\sigma_1)y+\sigma_4 r^4+\sigma_3 r^3+\sigma_2 r^2+\sigma_1 r+\sigma_0$
$=0$

[21]

を生成する。次に、ステップ５０４において、このシステムはｒに対して

$$\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2} を代入し、ここで$$

$$\sigma\sigma_3\left[\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}\right]^2+\sigma_1=\sigma_1+\sigma_1=0$$

であるので、線形項の係数はゼロである。したがって方程式２１は、

$$\sigma_4 y^4 + \sigma_3 y^3 + \left[(\sigma_3 * \sigma_1)^{1/2} + \sigma_2\right] y^2 + s,$$

[22]

となり、ここで「s」は方程式２１の定数項である。

この方程式を直接解くのではなくこのシステムはステップ５０６において、

$$\theta\theta(y) = \frac{y^4 * \gamma\left(\frac{1}{y}\right)}{s}.$$

[23]

の解を求める。

したがって、このシステムは、

$$\theta\theta(y) = \frac{y^4}{s}\left[\sigma_4 \frac{1}{y^4} + \sigma_3 \frac{1}{y^3} + \left[(\sigma_3 * \sigma_1)^{1/2} + \sigma_2\right]\frac{1}{y^2}\right] + s$$

[24]

または、

$\theta\theta(y)=y^4+\theta_2 y^2+\theta_1 y+\theta_0=0$

[25]

ここで

$$\theta\theta_2 = \frac{(\sigma_3 * \sigma_1)^{1/2} + \sigma_2}{s}$$

$$\theta\theta_1 = \frac{\sigma_3}{s}$$

$$\theta\theta_0 = \frac{\sigma_4}{s}$$

を解く。ステップ５０８においてこのシステムはまず方程式２５を因数分解して

、

$\theta(y)=(y^2+t^* y+u)^* (y^2+v^* y+w)=0$

[26]

とする。ここで方程式２５は因数分解できるものと仮定しているが、これはエラ

ーロケータ多項式の解がＧＦ（2^{2m}）内に存在するとするならば妥当な仮定である。

このシステムは方程式２６の項を展開して、

$\theta(y)=y^4+(t+v)y^3+(t*v+u+w)y^2+(t*w+v*u)y+u*w=0$

[27]

とし、この方程式の係数を方程式２５の係数に等しいものとおく（ステップ５１０）。

$t+v=0$

$t*v+u+w=\theta_2$

$t*w+v*u=\theta_1$

$u*w=\theta_0$

したがって、

$t=v$

$t^2+(u+w)=\theta_2$

$t*(w+u)=\theta_1$

$u*w=\theta_0$

ステップ５１２において、このシステムは次に唯一の未知数「ｔ」を持つ方程式を決定する。θ_2、θ_1およびθ_0はエラーロケータ多項式の係数の組合せであるの

で、既知であることを思い出されたい。したがって、このシステムは$u+w=\frac{\theta_1}{t}$

とおき、これをθ_2についての式に代入し、かつｔで乗することによって、方程式

$t^3+\theta_2 t+\theta_1=0$

[28]

を生成する。

この結果は、上のＢ節で説明した演算を用いて解くことができる二次多項式である（ステップ５１４）。特定的には、このシステムは変数を変え、

$$t=z+\frac{a}{z}\quad ここで\quad a=\theta_2$$

そして方程式２８は、

$$\left(z+\frac{a}{z}\right)^3+a\left(z+\frac{a}{z}\right)+\theta_1=0$$

となる。項を展開しかつまとめて、

$$z^3+\left(\frac{a}{z}\right)^2z+\frac{a}{z}z^2+\left(\frac{a}{z}\right)^3+a_3+\frac{a^2}{z}+\theta_2=$$

$$z^3+az+\frac{a^2}{z}+\frac{a^3}{z}+az+\frac{a^2}{z}+\theta_1=z^3+\frac{a^3}{z^3}+\theta_1=0$$

[29]

かつz^3で乗することによって、このシステムは、変数z^3を持つ二次方程式である方程式$(z^3)^2+\theta_1z^3+a^3=0$を生成する。

Ａ節の方法を用いて、このシステムは方程式２９の解を求める。

このシステムはこうして変数を変え、

$z^3=\theta_1 g$

[30]

とし、そして二次方程式は、

$\theta_1^2g^2+\theta_1^2g+a^3=0$

[31]

または

$$g^2+g+\frac{a^3}{\theta_1^2}=0$$

となる。もしトレース$\left(\frac{a^3}{\theta_1^2}\right)=0$ならば、方程式３１の解はＧＦ（$2^{2m}$）内に存在する。解が存在すると仮定すると、これらは、$\frac{a^3}{\theta_1^2}=\frac{\theta_2^3}{\theta_1^2}$を基底要素の線形結合に分解し、基底要素を対応する基底解と関連付けることによって、決定される。

一旦解が決定されると、システムはそれらのうち１つをたとえばg_0をz^3につ

いて式３０に代入し、図２の回路を用いてz^3の立方根z_0を決定する。このシステムは次に式

$$t = z + \frac{a}{z}$$

[32]

のzにz_0を代入して、これからt_0を決定する。

wおよびuを決定するために、このシステムはステップ５１６において、値t_0および式

$t^2+(u+w)=\theta_2$および

$u^*w=\theta_0$

を用いて、解としてuおよびwを有する二次方程式３３を生成する。

$(p+u)^*(p+w)=$

$p^2+(u+w)^*p+(u^*w)=$

$p^2+(\theta_2+t_0^2)^*p+\theta_0=0,$

[33]

このシステムは次に、A節の方法を用いて方程式３３の解を決定する。次にステップ５１８においてこれらの解p_0およびp_1を方程式２６の因数に代入して、二次方程式を生成する。

$y^2+t_0^*y+p_0=0$

および

[34]

$y^2+t_0^*y+p_1=0,$

そして、ステップ５２０においてA節の方法を用いて解y_0、y_1およびy_2、y_3について解く。方程式３３の解y_0、y_1、y_2およびy_3は$\theta(y)$の解であり、$1/y_0$、$1/y_1$、$1/y_2$および$1/y_3$は$\gamma(y)$の解である。次にこのシステムはステップ５２２において$1/y_0$、・・・$1/y_3$を式$x=y+r$に代入し、四次エラーロケータ多項式の解を決定する。最後に、このシステムはステップ５２４において、エラーロケータ多項式の解をコードワード内の位置と関連付ける。

この四次エラーロケータ多項式の解を決定する直接的方法は、チェンサーチを行なったりまたはm×mのマトリックスを操作したりするよりも迅速である。さらに、この方法においては、他の先行する既知のシステムにおいて使用される大きなルックアップテーブルが必要ない。

【図1】

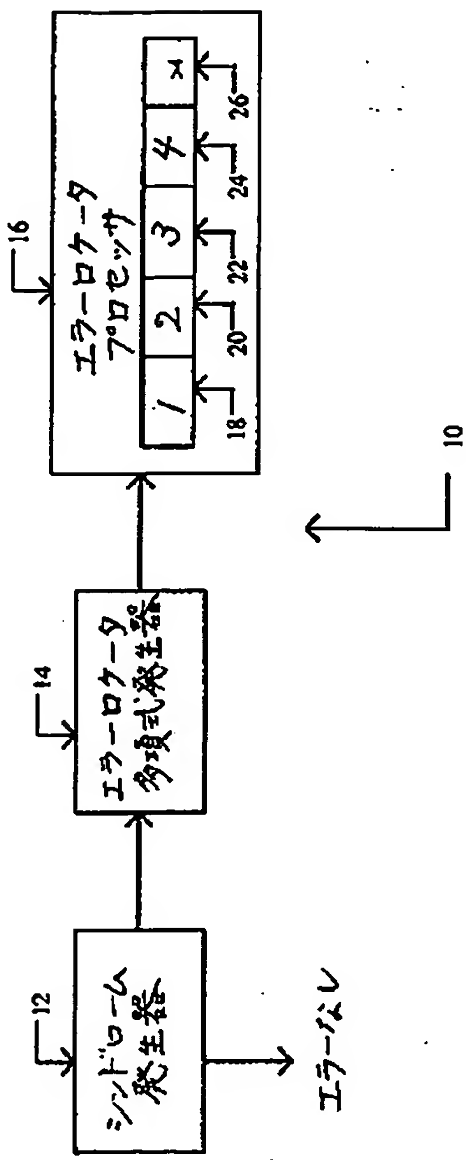
エラーロケータ
プロセッサ
16
1
2
3
4
x
18
20
22
24
26
エラーロケータ
多項式発生器
14
シンドローム
発生器
12
エラーなし
10

FIG. 1

【図2】

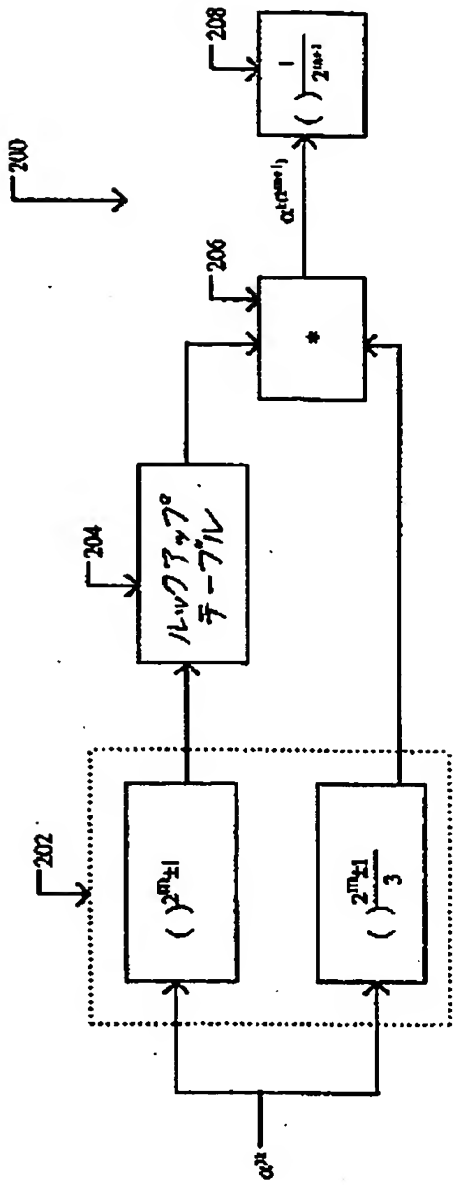

FIG. 2

【図3】

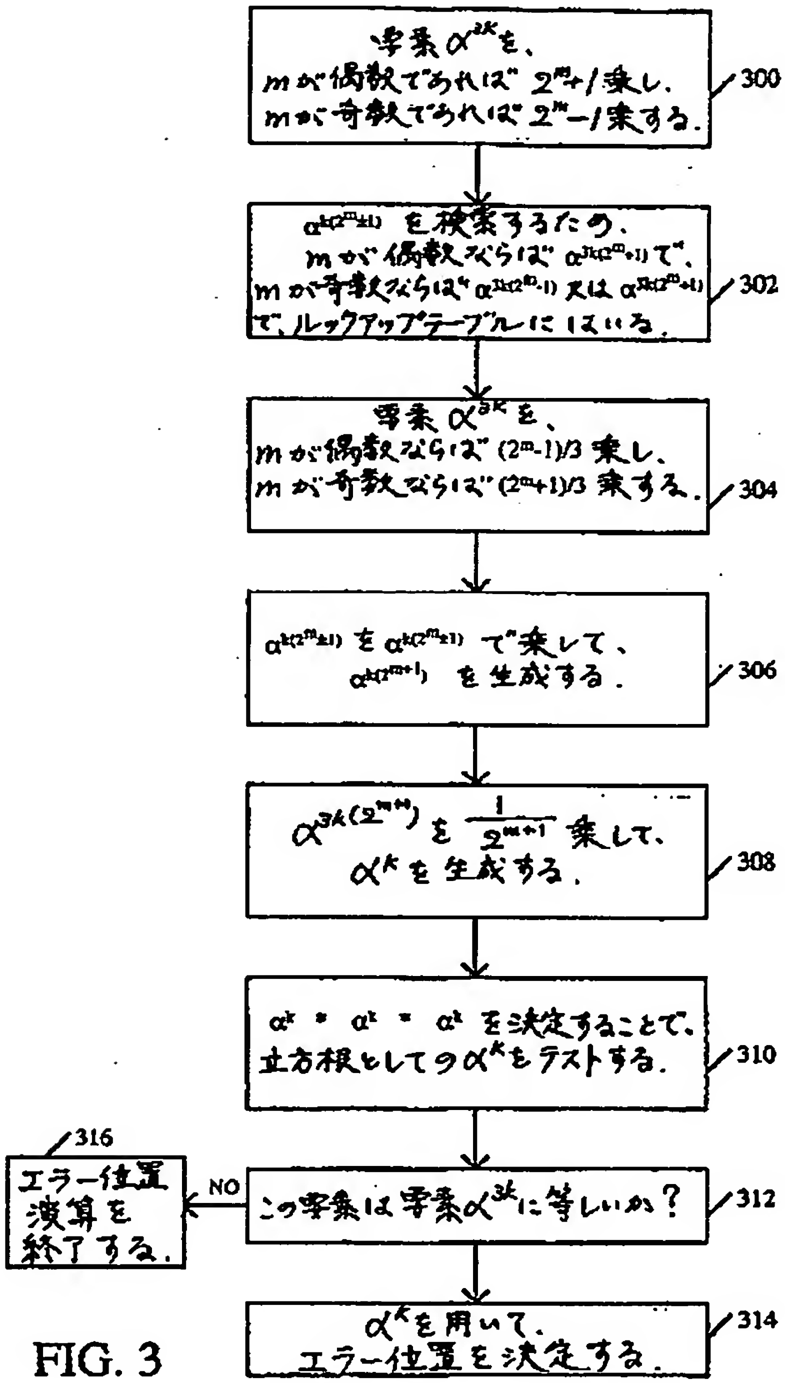
累乗α^{3K}を、
mが偶数であれば2^m+1乗し、
mが奇数であれば2^m-1乗する。
300
$\alpha^{3k(2^m\pm1)}$を検索するため、
mが偶数ならば$\alpha^{3k(2^m+1)}$で、
mが奇数ならば$\alpha^{3k(2^m-1)}$又は$\alpha^{3k(2^m+1)}$
で、ルックアップテーブルにはいる。
302
累乗α^{3K}を、
mが偶数ならば$(2^m-1)/3$乗し、
mが奇数ならば$(2^m+1)/3$乗する。
304
$\alpha^{3k(2^m\pm1)}$を$\alpha^{3k(2^m\mp1)}$で乗して、
$\alpha^{3k(2^m+1)}$を生成する。
306
$\alpha^{3k(2^m+1)}$を$\frac{1}{2^m+1}$乗して、
α^kを生成する。
308
$\alpha^k * \alpha^k * \alpha^k$を決定することで、
立方根としてのα^kをテストする。
310
この累乗は累乗α^{3k}に等しいか？
312
NO
エラー位置演算を終了する。
316
α^kを用いて、
エラー位置を決定する。
314

FIG. 3

【図4】

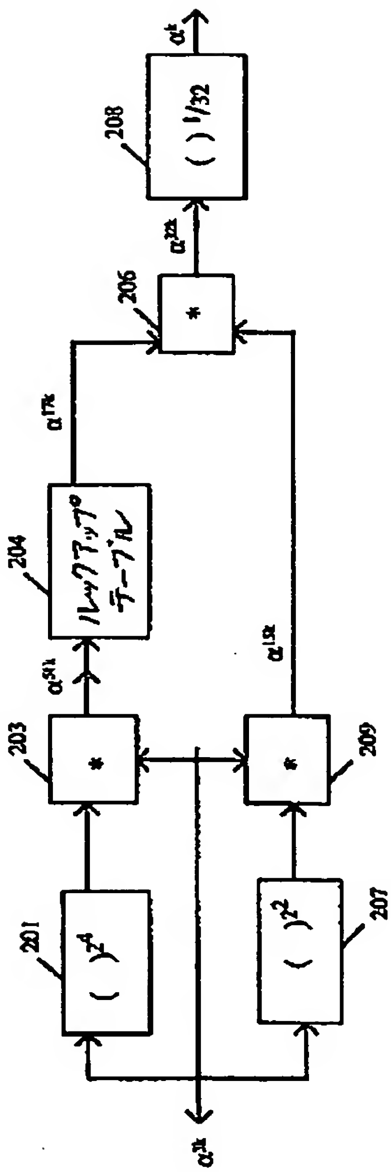

FIG. 4

【図5】

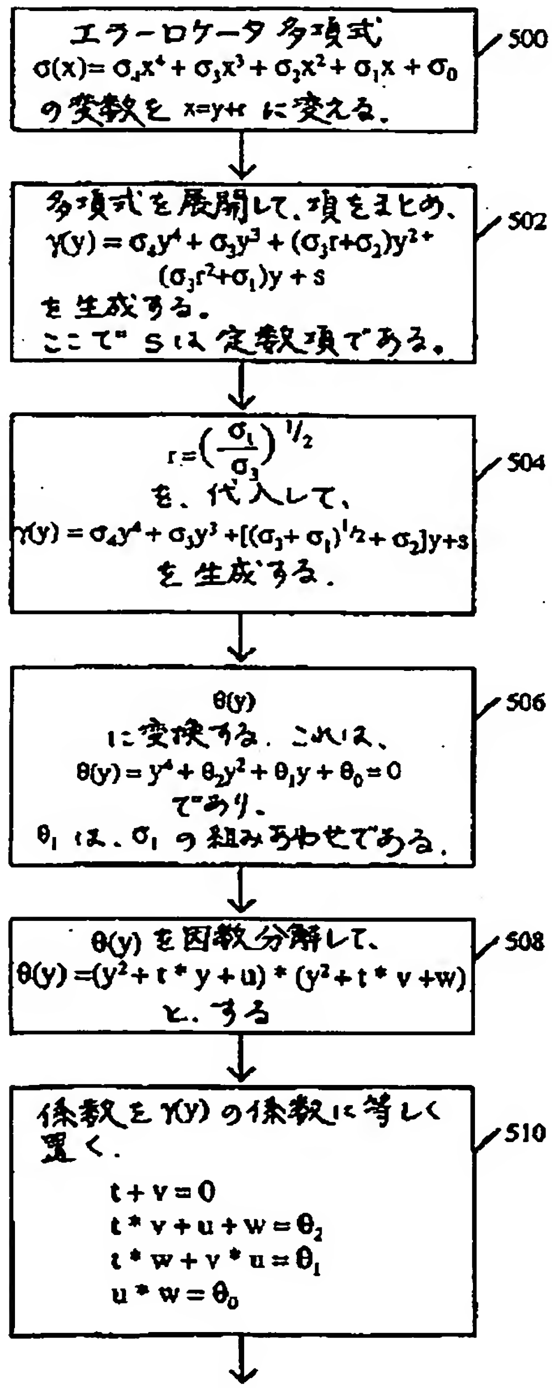
エラーロケータ多項式
$\sigma(x)=\sigma_4x^4+\sigma_3x^3+\sigma_2x^2+\sigma_1x+\sigma_0$
の変数を $x=y+r$ に変える。
500
多項式を展開して、項をまとめ、
$\gamma(y)=\sigma_4y^4+\sigma_3y^3+(\sigma_3r+\sigma_2)y^2+(\sigma_3r^2+\sigma_1)y+s$
を生成する。
ここで s は定数項である。
502
$r=\left(\frac{\sigma_1}{\sigma_3}\right)^{1/2}$
を、代入して、
$\gamma(y)=\sigma_4y^4+\sigma_3y^3+[(\sigma_3+\sigma_1)^{1/2}+\sigma_2]y+s$
を生成する。
504
$\theta(y)$
に変換する。これは、
$\theta(y)=y^4+\theta_2y^2+\theta_1y+\theta_0=0$
であり、
θ_1 は、σ_1 の組みあわせである。
506
$\theta(y)$ を因数分解して、
$\theta(y)=(y^2+t*y+u)*(y^2+t*v+w)$
と、する
508
係数を $\gamma(y)$ の係数に等しく置く。
$t+v=0$
$t*v+u+w=\theta_2$
$t*w+v*u=\theta_1$
$u*w=\theta_0$
510

FIG. 5

【図5（CONT）】

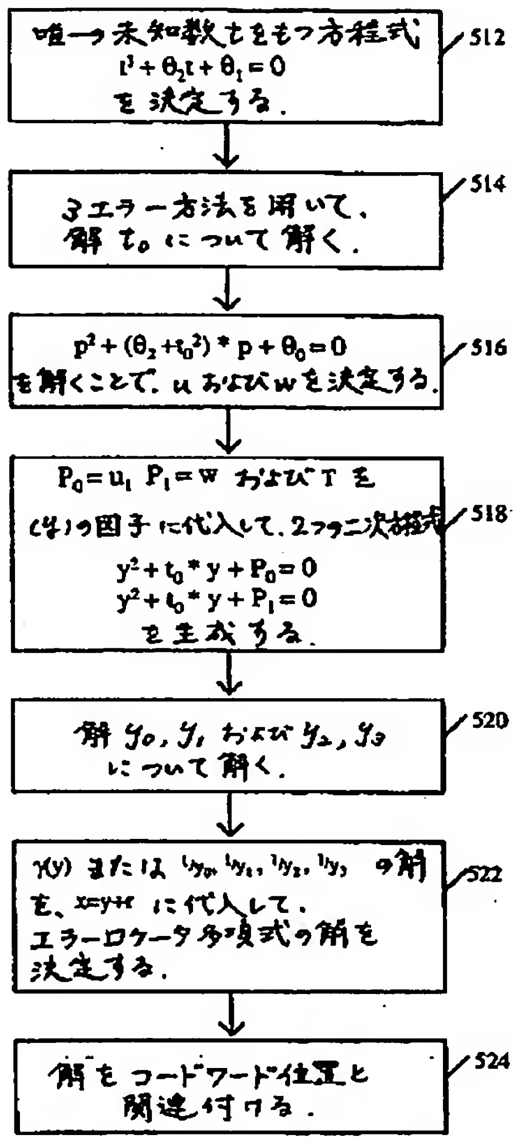

FIG. 5 (CONT)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/20547

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H03M 13/00
US CL :371/37.1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 371/37.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS Text
search terms 371/clas and (quadratic or root?)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- A	US, A, 4,567,594 (DEODHAR) 28 January 1986, col. 9 line 39 to col. 11 line 23.	4 -- 1-3, 5-7
A	US, A, 4,099,160 (FLAGG) 04 July 1978, col. 7, line 6 to col. 9 line 29.	1-7
A	US, A, 4,839,896 (GLOVER ET AL) 13 June 1989, col. 10 lines 60-69, col. 11 line 20 to col. 12 line 14.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 MARCH 1997	27 MAR 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer STEPHEN M. BAKER Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

【要約の続き】

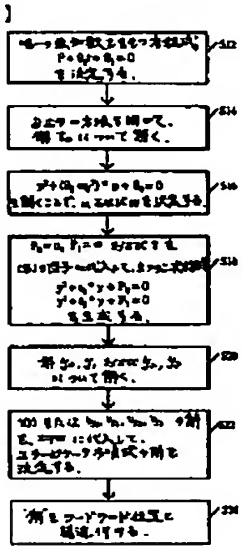

FIG. 5 (CONT)